UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,523	02/27/2004	Atsushi Minemura	NGB-36483	6891

116 7590 11/09/2007

PEARNE & GORDON LLP
1801 EAST 9TH STREET
SUITE 1200
CLEVELAND, OH 44114-3108

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
11/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/788,523	MINEMURA, ATSUSHI	
	Examiner	Art Unit	
	Amare Tabor	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *12 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to amendment filed on September 12, 2007.

2. Claims 1, 7, 8 and 11 are amended; and claims 12 and 13 are new.

3. Claims 1-13 are pending.

Response to Arguments

4. Applicant has amended claim 8 by including computer readable medium to over come the rejection of the claims under 35 USC 101. Therefore, the rejection has been withdrawn.

5. Applicant's arguments with respect to the rejection of claims 1-11 under 35 USC 112, second paragraph have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.

Response to Amendment

6. Applicant's arguments with respect to the original and amended claims have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 7, 8 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 7, 8 and 11 recite "*a terminal device having no secure information concealing area ...*" The detailed description of the invention mentions the underlined term (on page 4, lines 23-24; page 5, lines 4-5, page 6, lines 9-10; page 14, lines 19-20; and page 23, lines 10-11); however, the specification does not define what the "*no secure information concealing area*" is. Therefore, the claimed invention is rendered unclear and indefinite.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over "***DeTreville***" (US 6,609,199) in view of "***Barlow***" (US 6,484,259).

As per Claim 1, DeTreville teaches,

An application authentication system (see abstract) comprising: a terminal device having no secure information concealing area (*'open system'*; see FIG. 1-3; and for example, column 1, line 15 to column 2, line 30), said terminal device including an application (see *Applications 124* and *S/W Program(s)* in FIG. 2-3 and FIG. 11; and for example, column 4, line 64 to column 5, line 34) and application running means (see *Operating System 123* and *160* in FIG. 2-3 and FIG.11; and for example, column 4, line 64 to column 5, line 34); and a secure device connected detachably to said terminal device, said secure device for authenticating the application requesting access to the secure device (see *Portable Device 116* in FIG. 1-2; and for example, column 3, line 62 to column 5, line 34); wherein said secure device authenticates the application running means, and then authenticates the application based on a result of a process that the application running means execute on the application (see abstract and Summary of Invention; FIG. 13-15; and for example, column 21, line 65 to column 26, line 3).

DeTreville fails to teach secure device connected fixedly to terminal device. However, in the same field of endeavor, Barlow teaches secure device connected fixedly to terminal device (see abstract and *SC-CSP 246* in FIG. 3; and for example, column 8, lines 2-39). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to attach the secure device fixedly to the terminal, to provide a fast and easily accessible static security system (see column 1, line 20 to column 3, line 15 of Barlow).

As per Claim 7, DeTreville teaches,

A secure device (*'IC* device'; see *116* in FIG. 1-2; and for example, column 4) connected detachably to a terminal device, said secure device comprising: a card manager (see *'Authentication Application'* 130 in FIG. 2; and for example, column 4, line 64 to column 5, line 34) for executing a

process of authenticating the terminal device; and a card application for applying an authenticating process to an access request application stored in the terminal device; wherein the terminal device has no secure information concealing area (*'Open system'*), and wherein the card application authenticates the application based on a process that is applied to the application by the terminal device, then confirms that the process of authenticating the terminal by the card manager is completed, and then accepts an access request of the authenticated application (see abstract and Summary of Invention; FIG. 13-15; and for example, column 21, line 65 to column 26, line 15).

DeTreville fails to teach secure device connected fixedly to terminal device. However, Barlow teaches secure device connected fixedly to terminal device (see abstract and *SC-CSP 246* in FIG. 3; and for example, column 8, lines 2-39). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to attach the secure device fixedly to the terminal, to provide a fast and easily accessible static security system.

As per Claim 8, DeTreville teaches,

A terminal device including (*Computer 118* in FIG 2-3): an application running means (*Operating System 123* in FIG.2 and *160* in FIG.3); and an application stored in the terminal device (*Applications 124* in FIG.2 and *S/W Program(s) 166* in FIG. 3), wherein the terminal device has no secure information concealing area (*'open system'*), wherein the application running means calculates digest data of the application to request an access to a secure device after the fitted secure device authenticates the application running means, then authenticates the application by using the digest data, and then issues an access request to the secure device (see FIG. 1-6; and for example, column 3, line 60 to column 11, line 12).

As per Claim 11, DeTreville teaches,

An application authentication system comprising: a terminal device having no secure information concealing area (*'open system'*; see FIG. 1-3; and for example, column 1, line 17-column 2, line 30); and a secure device (*'IC* device'; see *116* in FIG. 1-2; and for example, column 4) connected detachably to said terminal device; wherein said terminal device includes 1) applications (see *Applications 124* and *S/W Program(s)* in FIG. 2-3; and for example, column 4, line 64 to column 5, line 34), and 2) application running means for running and authenticating the applications requesting access to the secure device (see *Operating System 123* and *160* in FIG. 2-3; and for example, column 4, line 64 to column 5, line 34), and wherein said secure device authenticates an application stored in the terminal device in order to permit access to said secure device, if the application is authenticated by application running means authenticated by said secure device (see abstract and Summary of Invention; FIG. 13-15; and for example, column 21, line 65 to column 26, line 15).

DeTreville fails to teach secure device connected fixedly to terminal device. However, Barlow teaches secure device connected fixedly to terminal device (see abstract and *SC-CSP 246* in FIG. 3; and for example, column 8, lines 2-39). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to attach the secure device fixedly to the terminal, to provide a fast and easily accessible static security system.

As per Claim 2 and 9, DeTreville teaches,

The application authentication system according to Claim 1, wherein the application running means (see *Operating System* 160 in FIG. 3) calculates digest data of the application to which an electronic signature is attached (see *Boot Log 158* in FIG.3 & 6; *Boot Block 162* in FIG.3 and *Signed boot block 180* in FIG. 4; and for example, column 5, line 36-column 9, line 25), and presents the digest data and the electronic signature to the secure device, and wherein the secure device verifies the electronic signature by using the presented digest data, and then authenticates the application if a verified result is normal (see column 9, line 25 to column 11, line 12).

As per Claim 3 and 10, DeTreville teaches,

The application authentication system according to Claim 1, wherein the application running means calculates digest data of the application and presents the digest data to the secure device, and wherein the secure device collates the presented digest data with digest data held in a database of the secure device, and then authenticates the application if a collated result is normal (see FIG. 5; *Equation 1* in column 9; and for example, column 5, line 35 to column 11, line 12).

As per Claim 4, DeTreville teaches,

The application authentication system according to Claim 3, wherein the application running means calculates digest data of the application and sends out a process request command to the secure device (see FIG. 5; *Equation 1* in column 9; and for example, column 5, line 35 to column 11, line 12), then wherein the secure device sends out first information to the application running means, then wherein the application running means encrypts the first information by using the digest data and sends out encrypted information to the secure device, and then wherein the secure device decrypts the encrypted information by using the digest data stored in a database of said secure device and then collates decrypted information with the first information (see FIG. 14-15; and for example, column 23, line 14 to column 26, line 3).

As per Claim 5, DeTreville teaches,

The application authentication system according to Claim 1, wherein the application running means verifies an electronic signature of the application to which the electronic signature is attached to authenticate the application, and wherein the secure device accepts an authenticated result of the application running means to authenticate the application (see FIG. 14-15; and for example, column 23, line 14 to column 26, line 3).

As per Claim 6, DeTreville teaches,

The application authentication system according to Claim 2, wherein the secure device 1) shares a second information with the application running means if the secure device authenticates the application running means, and 2) accepts a process request if the second information are added to the process request issued from the application that the secure device authenticates (see FIG. 13-15)

Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over "***DeTreville***" in view of "***Lee***" (US 7,000,249).

As per Claim 12, DeTreville teaches,

A terminal (*Computer 118* in FIG.2-3), comprising: an application storage unit (*Memory 112* and *Nonvolatile Memory* 136 in FIG.2-3) storing at least an application (*Applications 124 and S/W Programs 166* in FIG.2-3); an application execution environment verifying and executing said application; an Operating System (OS) verifying and invoking said application execution environment (see abstract, FIG.2-3 and FIG. 11); wherein the application execution environment transmits data including a hash of said application to the secure device and the secure device verifies a validity of the hash of said application (see FIG. 4-6; and for example, column 7, line 32 to column 11, line 12).

DeTreville fails to teach a Basic Input Output System (BIOS) verifying and invoking said OS; and a secure device verifying said BIOS. However, in the same field of endeavor, Lee teaches a BIOS verifying and invoking said OS (see FIG.1, 3-4); and a secure device verifying said BIOS (see abstract and FIG.1 and 5). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to verify BIOS and hash of application by using a secure device in order to protect public computers from attacks and prevent systems from revealing private information, that should be kept

secret, to unauthorized users (see column 1, line 22 to column 2, line 27 of DeTreville).

As per Claim 13, DeTreville teaches,

A method of verification of an application on a terminal (see abstract), comprising the steps of: verifying and invoking an application execution environment by the OS; verifying an executing the application stored in an application storage unit of the terminal by the application execution environment (see FIG.2-3 and FIG. 11); and transmitting data including a hash of said application to the secure device by the application execution environment; and verifying a validity of the received hash of the application by the secure device (see FIG. 4-6; and for example, column 7, line 32 to column 11, line 12).

DeTreville fails to teach verifying a Basic Input Output System (BIOS) by a secure device; verifying and invoking an Operating System (OS) by the BIOS. However, Lee teaches verifying BIOS by a secure device (see abstract and FIG.1 and 5); verifying and invoking an OS by the BIOS (see FIG.1, 3-4). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to verify BIOS and hash of application by using a secure device in order to protect public computers from attacks and prevent systems from revealing private information, that should be kept secret, to unauthorized users (see column 1, line 22 to column 2, line 27 of DeTreville).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
AU 2139

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100